RESEARCH ARTICLE

European Journal of Law and Political Science
www.ej-politics.org

An Assessment of International Law on the Use of Cyber-Espionage as a Substitute for Traditional Spying

Ayobamidele Joshua

ABSTRACT

Traditionally spying is an integral part of war, economic, and political sabotage among other things. In a bid to curb the incessant act of traditional spying which involves the act of physically and clandestinely crossing over to the countries where spying is to be carried out, various international conventions/instruments covering the act of traditional spying are of the moment. These include; the Hague Regulation of 1907, Vienna Convention of 1961, Geneva Conventions, United Nations Charter among others. In the same vein, Countries have enacted domestic laws to prevent the traditional spying/ clandestine acts within their territorial sovereignty. However, the 21st-century development in the field of technology and its use for a wind range of activities which include cyber espionage have questioned the effectiveness and relevance of international conventions and domestic laws on cyber espionage.

It is against this backdrop that this article embarks on the assessment of the conventions/instruments and domestic laws on cyber espionage. Precisely, it examines the assessment of countries' espionage laws and their relevance to cyber espionage among countries, the assessment of international law and its relevance to cyber espionage, the assessment of customary international law on cyber espionage, and recommendations. Accordingly, it concludes that a holistic assessment of cyber espionage reveals that the applicability of extant international law to it like traditional spying is uncertain.1.

Keywords: Countries, Cyber Espionage, Information, International Law, Traditional Spying.

Published Online: September 20, 2022

ISSN: 2796-1176

DOI: 10.24018/ejpolitics.2022.1.4.21

A. Joshua *
Adekunle Ajasin University, Nigeria.
(e-mail: ayobamijoshua0312@gmail.com)

Corresponding Author

I. INTRODUCTION

The practice of spying as a profession was a lucrative one since primitive times. Greek history has it that three spies from Greece were captured by Persian soldiers in the Sardes region who were looking for secret information about the power of the Persian army (Richmond, 1998). This is, therefore a confirmation that espionage is a veritable tool in the hands of soldiers in prosecuting a war, even before the advent of technology. Traditional spying which is otherwise known as conventional espionage is, therefore, a process involving human agents or technical means to acquire information normally not publicly available (The MI5, n.d.). It involves a systemic arrangement whereby top and classical military or economic information are accessed clandestinely through the direct human effort of crossing the border to another country to access such information. In a bid to ensure that spies captured in the course of carrying out such clandestine, especially in times of war are treated humanely, various international instruments/conventions were established and acceded to by countries (The Hague Convention Respecting the Laws and Customs of War on Land, article. 29.; Additional Protocol to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts, article 46 (2)).

It is imperative to point out that where such clandestine acts are carried out in a time of peace, international law is practically inapplicable. It, however, regulates some activities related to peacetime espionage (Buchan, 2016). This is where Countries under their respective Law of Armed Conflict (LOAC) to prohibits the use of espionage to gather or obtain information within their territories illegally (Nigeria's Manual on Laws of War, 1994; Canada's LOAC, 2001; United Kingdom's LOAC, 2004; The Russian Federation's Regulation on the Application of International Humanitarian Law, 2001).

In the 21st century, the traditional concept of espionage whereby a State dispatches a spy into the physical territory of another state to clandestinely access and obtain confidential information has become archaic, unpopular and prone to exposure before such an agent completes the mission. It is worthy of note that LOAC of States carries one to ten years imprisonment as punishment for such traditional spying (Bosnia and Herzegovina's Criminal Code, 2003, article 2; Croatia's Criminal Code, 2007 as amended in 2006, articles 2 and 5), and death in some States (Morocco's Military Justice Code, 1956; The Central African Republic's Penal Code, 2010). In its current development, spy activities are carried out using the latest

technology so that they can obtain confidential information easily, quickly, and without being known from the destination country (Setiawan, 2016). Cyber espionage has been used by countries to access military, economic, or infrastructural information from other countries illegally thereby causing monumental problems to countries that originally owned such information.

The important question, therefore, is to what extent can it be said that international law that regulates traditional spying can adequately regulate cyber espionage, considering 21st century encrypt and decrypt means of transferring and deciphering information without having to physically cross the border as an agent to access military, economic or infrastructural information clandestinely. This article assesses the international law on the use of cyber espionage as a substitute for traditional spying to contribute to the discussion on the relevance or otherwise of the existing international laws to the new phenomena such as cyber espionage. The article is structured to have the following sub-division; assessment of Countries' espionage laws on cyber espionage, assessment of the international law on cyber espionage, assessment of customary international law on cyber espionage, recommendations and conclusion.

II. Assessment of Countries' Espionage Laws and Their Relevance to Cyber Espionage among Countries

International law allows each Counrty to put measures in place to prevent clandestine acts within its territorial integrity, especially during armed conflict. The golden provision in this regard is Article 51 of the United Nations Charter which provides that:

[n]othing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security (Charter of the United Nations and Statute of the International Court of Justice, 1945).

Countries have leveraged article 51 of the UN Charter to enact their respective laws to prohibit and punish espionage committed within their borders. This article takes a cursory look at some of the Countries' laws on traditional spying with the punishments attached for such espionage acts.

a. The United States Manual for Military Commission (USMMC) has this to say on espionage:

Text any person to this chapter who in violation of the law of war and with intent or reason to believe that it is to be used to the injury of the United States or the advantage of a foreign power, collects or attempt to collects information by clandestine means or while acting under false pretence for the purpose of conveying such information to an enemy of the United States, or one of the co-belligerents of the enemy, shall be punished by death or such other punishment as a military commission under this chapter may direct (USMMC, 2010).

In the same vein, the Uniform Code of Military Justice (UCMJ) states that:

> The sentence of death shall be passed on any person captured in the act of proven to be lurking as a spy in or about any place, vessel, or aircraft, within the jurisdiction of any of the armed forces, or in or about shipyard…or any place or institution engaged in aid of the prosecution of the war by the United States, or elsewhere (UCMJ, 1951, article 106).

b. Morocco's Military Justice Code (MMJC) states that:

> Any enemy who, in disguise, intrude into one of the locations listed in the preceding article [area of war, military post or establishment, work, camps, bivovacs of quarters of an arm] is punished by death (MMJC, 1956, (n7)).

c. The Democratic Republic of Congo's Military Penal Code (DRCMPC) states that:

> Guilty of escfpionage and punished by death is everyone who is the perpetrator of the acts of delivery to foreign power materials, constructions, equipment, installations, appliances, objects, documents, computer data or files, whose exploitation, divulgation, or reunion is of a nature to endanger the fundamental interests of the nation or other material devoted to national defence (DRCMPC, 2002, article 129).

d. The Cote d'ivoire's LOAC Manual states that:

> Civilian saboteur not wearing uniform do not receive that protection and risk being treated as spies, They can be brought to justice in conformity with the laws of the force which has captured them and can incur death penalty. They can, however, not be punished without fair trial (CDLOACM, 2007).

It is vital to point out that the laws of the countries cited above-prescribed death as a penalty for an act of traditional spying otherwise called traditional espionage committed within their territorial integrities. However, there are countries where their laws prescribed several years as imprisonment for the act of traditional espionage committed within their borders. These Countries include:

a. Bosnia and Herzegovina's Criminal Code (BHCC) states that:
   Whoever obtain secret data with an aim of disclosing or delivering it to foreign Country, foreign organisation or person in the service thereof shall be punished by imprisonment for a term of between one and ten years (BHCC, 2003, (n6) 4).
b. Switzerland's Military Criminal Code (SMC) states that:
   A person who has gathered military information on Swiss territory for a foreign State to the detriment of another foreign State or has organised such service is to be punished with three years or more imprisonment or with a monetary penalty (SMC, 1927; Amended, 2007).
c. Croatia's Criminal Code (CCC) states that:
   Whoever collects data, objects, documents or information which are a state secret with an aim of making them accessible to a foreign state, and organisation or a person working for them shall be punished by imprisonment for one to three years (CCC, 2007, (6) (2)).
d. Nigeria's Manual on Laws of War (NMLW) states that:
   Lawful punishment under the municipal law may be imposed upon individuals who engage in espionage or treason when they are caught by the enemy (NMLW, 1994).

This article opines that all these laws are enacted with belief that espionage acts could only be perpetrated when an agent of a Country physically goes to another country to access information clandestinely. The Countries whose information is been or is likely to be clandestinely accessed are prepared to protect all information within its border, hence the need for an espionage law. The United States Espionage Act (USEA) prohibits interference with military operations or recruitment, prevents insubordination in the military, and prevents the support of the United States enemies during war (USEA, 1917, Rule 107). In *Gorin v United States* ([1941] US 19 312) the accused was charged with copying, taking, making and obtaining documents, writings, and notes of matters connected with the national defence and transmit same to the Soviet Union. He was tried and sentenced to six years imprisonment having been guilty under Espionage Act ([1941] US 19 312). It is, however, worthy of note that an assessment of the Espionage Act reveals that it is no longer relevant in the light of the 21st espionage known as cyber espionage.

The writer reasons that careful assessments of the laws enacted by Countries to discourage, prevent, or punish traditional spying is incapable and cannot prevent cyber espionage in the 21st century. In its current development, spy activities are carried out using the latest technology so that they can obtain confidential information easily, quickly, and without being known from the destination country (Heriyanto, 2019, (n 8) 106).

A further assessment of the Countries' traditional spying law reveals that it is targeting citizens of another country that entered a Country and clandestinely obtained information with or without the aid of the home Country's citizens. However, 21st-century spies do not need to physically cross into the territory of another country before assessing information clandestinely. In June 2013, cyber espionage was thrust firmly into the international spotlight when Edward Snowden, a former contractor for the United States National Security Agency (NSA), disclosed through Wikileaks thousands of classified documents to several media companies including The Guardian and The New York Times (Buchan, 2016, (n 4) 2). The documents were alleged to reveal that the NSA had been engaged in a global surveillance programme and at the heart of this surveillance programme was the collection of confidential information that was being stored in or transmitted through cyberspace (Buchan, 2016, (n 4) 2). In particular, the allegations were that the NSA had been engaged in a sustained and widespread campaign of intercepting and monitoring private email and telephone communications (Buchan, 2016, (n 4) 2). The effect of this is that Edward Snowden could not be tied to the US Espionage Act for the over simplistic reason that the Act only applied to traditional spying even though Edward Snowden had run for his life.

Countries have developed a system whereby spies' teams are created, equipped, funded, trained and retrained to carry out cyber espionage for them. In February 2013 the Mandiant Report identified China as a persistent perpetrator of cyber espionage through an entity known as Unit 61398 which was incorporated into the People's Liberation Army (Mandiant Report, 2013). The report suggests that Unit 61398 is responsible for organising and instigating a massive cyber espionage campaign against other states and non-state actors, looking to exploit vulnerable computer systems to access sensitive and confidential information to bolster China's position in the international political and economic order (Mandiant Report, 2013).

China is reported known for its specialisation in the act of cyber espionage through the use of various hacker groups which include Titan Rain, Ghost Net, Moon Light Maza among others. In 2003, the US experienced monumental cyber espionage from Titan Rain that targeted the National Security Agency (NSA), the Department of Defence (DoD) and private institutions (Arthur, 2005). The clandestine act was believed to have been backed by the Chinese government (Arthur, 2005). Additionally, in 2007 Titan Rain carried out a clandestine act of infiltration of the US and the United Kingdom (UK) governmental departments' digital documents such as the US military DoD, the UK foreign and commonwealth digital office (Corinne *et al.*, 2015). The act was reported to have been carried out by a group (Titan Rain) that

secretly has the Chinese government's backing (Corinne *et al.,* 2015). In the same vein, in 2009 it was revealed that a large-scale spying network had attacked a significant number of government departments and strategic target including the Tibetan community (Moore, 2009). Again, a forensic instigation revealed that the clandestine act was perpetrated by a group called Ghost Net back rolling by the Chinese government. It is, however, noteworthy that China is not the only country that carries out cyber espionage as other Countries in Europe and Asia are involved in such clandestine infiltration. An instance is Edward Snowden that worked as an ICT spy for the US government before defecting away (Buchan, 2016, (n 4) 2).

Ordinarily, any State that allows any organisation to use its territory for any activities (cyber espionage) would take full responsibility under international law so far as the State acknowledges and recognises such organisation or person. International Law Commission's (ILC) 2001 Articles on Responsibility of States for Internationally Wrongful Acts (Draft Articles) states that:

> the conduct of a person or a group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct (Article 8of the ILC on Articles on Responsibility of States for Internationally Wrongful Acts, 2001).

However, ILO remains in the realm of a document because States have developed ways of circumventing the international instrument by refusing to align themselves with such person or group of persons even when it is crystal clear that such person or group of persons is working for the country or working on the soil of a Country that put up denial. The case of South China Sea Arbitration between the Philippines and China before the Permanent Court of Arbitration (PCA) (Philippines v. China [2013] PCA 19; Award of 12 July 2016) revealed how cyber espionage could be carried out without attracting any responsibility to a Country whose territory was used to perpetrate such a clandestine act. In that case, the Philippines challenged China's maritime claims and activities in the South China Sea (Philippines v. China, 2013 PCA 19). Surprisingly, on the third day of hearing the case in 2015, the PCA's website located at its Peace Palace in Hague was clandestinely infiltrated leaving the page infected with malware luring unsuspecting online visitors (Healey & Piiparinen, 2015). According to Benatar forensic investigations led an IT security company to conclude that an actor based in China had targeted the computer systems of groups involved in the maritime spat (Benatar, 2019). China or the other hand did not admit responsibility for this act but claiming that it has no nexus with any group of person or commission any person or group to carry out such clandestine act.

The 2007 Russian cyber attackers were suggested to have been responsible for cyber espionage on Estonia in which for about a month, Estonia's internet websites were flooded with pings and network-clogging data (Connell &Vogler, 2017). Thereby forcing most sites to either shut down or sever their international connections (thus rendering much of the country's ability to communicate or share information efficiently with the outside world unusable) for weeks (Connell &Vogler, 2017). It becomes difficult for North Atlantic Treaty Organisation (NATO) to invoke its article 5 and come to the aid of Estonia when Estonia calls for help. This is because the cyber attack through the work of the cyber-spies could not be traced to Russia even though all cyber investigation is irresistibly pointing to Russia as the perpetrator through its hackers.

Similarly, in 2008 during Russia and Georgia war, Russian hackers attack government websites in the city of Gori in eastern Georgia, along with news websites, just before Russian air attacks on the city (Mann, 2008). Russia however, denies ever using cyber attack alongside conventional warfare against Georgia (Connell & Vogler (n 29), 2017), because the evidence is unclear whether Russia was involved in the shutdown of Georgian websites or whether the attacks can be attributed to non-state actors (Swaine, 2008). Even though Smith suggests that Russian hacktivist websites, such as *stopgeorgia.ru*, provides lists of Georgian sites to attack, along with instructions, downloadable malware, and after-action assessments (Smith, 2012). It is opined that Russian Federation is fully aware of the international responsibility placed on her by the ILO that is why its ensure that the hacktivist clandestine act is not traceable to its territory or at least tracing the hacktivist clandestine act to its territory remains unclear/doubtful.

It is argued that all the ICT clandestine acts of infiltrating and accessing 'classified documents' from a Country through a group of persons or hacktivists for another Country are possible due to the use of 21st-century internet prowess. Unfortunately, the extant espionage laws of Countries are ineffective when it comes to applying them to cyber espionage and no Country is ready to admit that its territory as a base for carrying out cyber espionage, yet the incidence of cyber espionage is unabated. It is, therefore, the opinion of this article that the extant espionage laws of Countries are only applicable to traditional spying which has been circumvented severally through the use of ICT to carry out espionage.

III. Assessment of International Law and Its Relevance to Cyber Espionage

There is no certainty as to the international law regulating cyber espionage, at best international treaties are applicable through analogous principles. However, due to the growing rate at which Countries are using ICT to perpetrate espionage, the UN expressed its opinion through the UN Secretary-General when it says:

> Few technologies have been as powerful as information and communications technologies (ICTs) in reshaping economies, societies and international relations. Cyberspace touches every aspect of our lives. The benefits are enormous, but these do not come without risk. Making cyberspace stable and secure can be achieved only through international cooperation, and the foundation of this cooperation must be international law and the principles of the Charter of the United Nations (GGE Report, 2015).

The UN expression on the use of ICT has double phases in which of it it's the risk which comes which it. Cyber espionage, therefore, sits squarely in the risk phase since it is a criminal act of clandestinely accessing information from another Country's ICT base. A fundamental question is to what extent can it be said that international law applies to cyber espionage considering the volume of international law applicable to traditional spying. Buchan however, insists that whilst cyber espionage is not specifically regulated by international law it may be nevertheless unlawful when appraised against general principles of international law (Buchan, 2016, (n 4) 3). This work opines that *Lotus* (Lotus Case (France v Turkey), 1927) principle gives a Countrywide range of discretionary power under international law but limit in certain probative rule and the absence of such rule States are free to adopt a certain principle that is suitable and best (Lotus Case (France v Turkey), 1927, paras 18-19) explains basis for applying exiting international law to cyber espionage analogously.

However, various principles have been developed over time to have a uniform approach under international law that is applicable in protecting Countries' information data from cyber espionage. They are; the principle of territorial sovereignty (Corfu Channel United Kingdom of Great Britain and Northern Ireland v Albania, 1949), the principle of non-intervention (Nicaragua (Nicaragua v United States of America), 1989), and the prohibition against the use of force (UN Charter article 2(4)).

A. The Principle of Territorial Sovereignty

Under international law, territorial sovereignty is what distinctively define and separate an independent Country from another. It includes land, internal waters, territorial sea, archipelagic waters, and national airspace or platforms (for example aircraft, satellites or vessels) (United Nations Convention on the Law of the Sea, 1982. part 2 article 2). Thus, an unauthorized entry into and presence in a state's sovereign areas of a foreign organ, in the form of for example an agent who acts in official capacity, would violate the territorial sovereignty of the State intruded upon (Shoshan, 2014). On territorial sovereignty, International Court of Justice (ICJ) in *Corfu Channel* case (Corfu Channel (n 49)) puts it this way; '[b] etween independent States, respect for territorial sovereignty is an essential foundation of international relations'. In the assessment of whether infiltration of 'classified documents' of a Country through the manipulation of the ICT without physically entering such Country under clandestine infiltration amount to the cyber espionage of violation of territorial sovereignty. This question was answered in the affirmative in *Islands of Palmas case* (Islands of Palmas (Netherlands v US), 1928) where it was held that:

> Because data is stored on servers, and servers are included in the definition of cyber infrastructure, this means that if data intruded upon is located on the target state's territory the target state has a right to exercise 'sovereign prerogatives' over that data.

Similarly, damages is irrelevant and the mere fact that a State has intruded into cyber infrastructure of another State should be considered an exercise of jurisdiction on foreign territory, which always constitutes a violation of the principle of territorial sovereignty (Heintschel von Heinegg, 2013). Shoshan suggests that an application of sovereignty results in the conclusion that a state that enjoys sovereignty over the territory where a server is located, also has the right to decide over access to that server and the data stored in the server (Shoshan, 2014, (n 53) 34).

The article argues that even though infiltration of territorial sovereignty of Country amounts to violation under international law (Islands of Palmas, 1928, n. 55). It is, however, reasons that applying such international law to cyber espionage leaves much to be desired. The major impediment to such application is the 'principle of denial' which allows an alleged cyber infiltrator to denied such cyber espionage, even though there might be investigation pointing to emanation of clandestine act from its Country. Upon a forensic investigation that revealed that the US carried out cyber espionage on Brazil, the Brazilian former President Dilma Rousseff, boycotted a scheduled meeting with the formal US, Obama in Washington DC but proceeded to address UN General Assembly on the clandestine act of the US (The Guardian, 2013). She states that:

intrusion [and] [m]eddling in such a manner in the life and affairs of other countries is a breach of international law [and] as such an affront to the principles.

that must guide the relations among them, especially among friendly nations. A Country's sovereignty can never affirmed itself to the detriment of another Country' sovereignty (The Guardian, 2013).

Even though the Brazilian former President Dilma Rousseff objected to such clandestine infiltration against her Country and demanded for explanation, apologies and assurance that such act will never repeat itself (The Guardian, 2013). The US neither apologise nor make any promise because there is not concluding acceptability by the US that such act is from it even though Snowden report pointed otherwise The writer insists that the applicability of international law on territorial sovereignty on cyber espionage would at best be by analogy which many Countries would not subscribe to. This article therefore, agrees with the contention of Buchan that acts of cyber espionage that intrudes upon the cyber infrastructure of a state for intelligence gathering constitutes a violation of the principle of territorial sovereignty (Buchan, 2016, (n 4) 8).

B. The Principle of Non-Intervention

This principle depicts that every Country must be at liberty to take decision on its own on all matters within its border for its good without external involvement or be at behest of Country for whatsoever reason. This view is corroborated by the international law through *Nicaragua case* (Case Concerning the Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v United States of America), 1986), ICJ elucidates on the principle of non-intervention that:

> [B]earing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely. One of these is the choice of a political, economic, social and cultural system, and the formulation of foreign policy. Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones. The element of coercion, which defines, and indeed forms the very essence of, prohibited intervention, is particularly obvious in the case of an intervention which uses force, either in the direct form of military action, or in the indirect form of support for subversive or terrorist armed activities within another State.

In accessing this principle based on cyber espionage, this article reasons that since unwelcome intervention of a Country in another Country's home affairs could be through element of coercion, the traditional meaning of principle of non-intervention as enunciates in *Nicaragua case* may be far from been relevant to cyber espionage. It is on that basis that its clear that the intrusion that cyber espionage constitutes can be seen neither as coercion nor dictatorial interference in the target state (Shoshan, 2014, (n 53) 45).

The article is not unmindful of the fact that cyber espionage is a criminal offence in the context of the domestic law of Countries. For illustration, it can perhaps be contended that whilst the systematic accessing of information belonging to senior state officials (such as the Head of State) is likely to exceed the *de minimis* threshold, the one-off accessing of innocuous electronic correspondence of a low-ranking civil servant is unlikely to be considered sufficiently serious to justify the engagement of international law. (Buchan, 2016, (n 4) 16).

C. The Prohibition against the Use of Force

The systemic approach of cyber espionage has no nexus with the use of force. Lin, however, suggest that it may from a technical standpoint be very difficult to distinguish between a cyber attack and a cyber exploitation (for example in the form of cyber espionage), because both begin with taking advantage of a vulnerability in the targeted system (Lin, 2010). It is important to point out that analogously, article 2(4) of the UN Charter[1] serves as haven for cyber espionage even though the Charter did not define what amount to the use of force. Countries, however, agree that a variety of unfriendly actions including espionage do not reach the threshold of use of force (Lin, 2010, (n 66) 71). It is, therefore, argue that various act of cyber espionage carried out by China does not amount to Chinese use of force on the US (Arthur, 2005, (n 28)). Dinstein insists that the specific means-kinetic or electronic-used to conduct the action does not matter; instead, what matters is whether the final result involves threat or occurrence of violence (Dinstein, 2011).

Therefore, assessment of use of force has being analogously applicable to cyber espionage would create confusion and make international diplomatic relations unfriendly because article 2(4) of the UN Charter will be taken bound its only interpretation which is applicable to use of armed force.

[1] It provides that 'All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or any other manner inconsistent with the purposes of the United Nations.'

IV. Assessment of Customary International Law on Cyber Espionage

Customary International law (CIL) emanates from the consistency in the Countries practice provided it has nexus with the legal obligation requires of them. Precisely, CIL are entrenched in two elements, viz; State practice and *opinion jurissive necessitates*. The State practice could be embedded in State actions, published government materials, official government statements, domestic laws, and court decisions that detail actual practice (Restatement of the Law, Third, Foreign Relations Law of the United States [1987] section 102). The *opinion juris*, belief that a State activity is legally obligatory, is the factor which turns the usage into a custom and renders it part of the rules of international law (Ayalew, 2015). Evidence of *opinio juris* is primarily shown through statements of belief, as opposed to statements about State practice, such as treaties or declarations (Roberts, 2011). Smith expounds that because espionage is such a fixture of international affairs, it is fair to say that the practice of states recognizes espionage as a legitimate function of the state, and therefore it is legal as a matter of customary international law (Smith, 2007). Heriyanto explains that obtaining information from the other states by employing the methods of cyber espionage is a violation to the Vienna Convention 1961 (Heriyanto, 2019).

It is, however, unending discussion as to whether CIL applies to cyber espionage. Where a Country accused of another of committing cyber espionage on its territorial sovereignty and accused Country objected to such accusation, affirming such act as forming State practice under international law might be difficult. This article reasons that this is what is obtainable among Countries when there are accusations and counter accusations of cyber espionage. The international reaction to the Snowden cyber revelation is to the effects that the practice of cyber espionage is incompatible with international law, though political or moral grounds (Buchan, 2016, (n 4) 19).

V. Recommendations

A. There Should Be Countries Responsibility

Cyber espionage involves the use of high-tech to clandestinely access information illegally from a Country whose cyber technology is inferior to the infiltrator. It is based on this that weaker Countries especially in the third world Countries are prone to cyber espionage from technologically advanced Countries. Therefore, it is recommends that Countries whose territorial integrity is accused of been save haven for cyber espionage should be ready to accept responsibility of cooperating with the international investigation to expose such perpetrator. This would facilitate and maintain cordial diplomatic relations and keep international obligations alive.

B. Creation of International Instrument on Cyber Espionage

As noted in this article, the entire international instruments in formed of Conventions, domestic laws of Countries and cases which ICJ adjudicated on are purely applicable to traditional espionage as illegal act. The effect of this is that Countries find it easy to perpetrate cyber espionage on each other through the use of cyber infiltrators and turn around to denied having any nexus with such cyber infiltrators. Additionally, it makes attributions of conduct to them in line with articles 1 and 2 of the ILC Draft impossible thereby resulted into unending debate on the applicability of the extant laws international laws to cyber espionage as contained in this article. This article therefore, recommends convention under the auspices of the UN to address cyber espionage and other cyber related matters. It is imperative to point out that NATO had already started this by including cyber espionage in its Tannin Manual and the UN should leverage on this.

C. Creation and Upgrading of Cyber Power

The need for the creation of cyber command for each Country cannot be over emphasis. This becomes imperative since cyber espionage could not be said to have fall within the purview of use of force, yet a Country must protect itself from clandestine act of another Country. The necessity for the creation of cyber command especially for African Countries becomes apparent due to unwillingness of Country whose territorial sovereignty serves as home for the perpetrator of cyber espionage to accept responsibility under international law. Therefore, the creation of cyber domain would facilitate encryption of 'classify documents,' protection of cyber infrastructures, concealment of military codes for manufacturing of weapons, keeping of national top secrets and information. In the same vein, Countries that have created cyber command should not relent but move on to retrain their cyber combatants on cyber espionage, carry out additional research on new methods of cyber espionage and how to prevent it or stop it.

VI. Conclusion

This article assesses the traditional spying otherwise called conventional espionage to ascertain if the extant international law could be an antidote to the clandestine act of cyber espionage. As pointed out in

this work, the assessment of Countries' domestic laws, international laws as well as ICJ position on international cases which metamorphosis to CIL could not be said to have adequately relevance to the incidence of cyber espionage. At best, the extant international law can only apply to cyber espionage analogically due to the act of using ICT to commit cyber espionage.

It is, therefore, expected that international community would act to mitigate act of cyber espionage so that international diplomatic relations is not destroy beyond repair and the time to act is now.

REFERENCES

Arthur, C. (2005). Google the Latest Victim of Chinese State-Sponsored Cyberwar. *The Guardian*. Retrieved 30 June 2022 from http://www.guardian.co.uk/technology/2010/jan/14/google-hackingchina-cyberwar.

Ayalew Y. E. (2015). Cyber Warfare: A New Hullaballoo under International Humanitarian Law. *Beijing Law Review*, 6, 218.

Benatar, M. (2019). Cyber Espionage in Inter-State Litigation. In Hélène Ruiz Fabri (ed.) *International Law and Litigation. A Look into Procedure.* Nomos.

Bosnia and Herzegovina's Criminal Code (BHCC). (2003).

Buchan, R.J. (Accepted: 2016) The International Legal Regulation of Cyber Espionage. In: Osula, A.-M. and Rõigas, H., (eds.) *International Cyber Norms: Legal, Policy & Industry Perspectives*. NATO CCD COE Publications , Tallinn, Estonia, pp. 65-86. ISBN 9789949954469 9789949954476.

Canada's LOAC. (2001).

Case Concerning the Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v United States of America) (Merits). (1986). ICJ Rep 14, para 205.

CDLOACM. (2007).

Charter of the United Nations and Statute of the International Court of Justice. (1945).

Connell, S. and Vogler, S. (2017). Russia's Approach to Cyber Warfare. CNA Analysis and Solution Publishing, Moscow.

Corinne, J. N., Glorioso, L., Rosaria, M. (2015). NATO CCD COE Workshop Ethics and Policies for Cyber Warfare. Magdale College, Oxford Report. www.ccdcoe.org.

Corfu Channel United Kingdom of Great Britain and Northern Ireland v Albania. (1949) ICJ Rep 1 35.

Croatia's Criminal Code (CCC). (2007).

Dinstein, Y. (2011). *War, Aggression and Self-Defence*. 5th edition Cambridge University Press, Cambridge.

DRCMPC. (2002).

GGE Report. (2015). Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/70/174, 22 July 2015, para. 4.

Healey, J. and Piiparinen, A. (2015). Did China Just Hack the International Court Adjudicating Its South China Sea Territorial Claims? *The Diplomat*. Retrieved 30 June 2022 from http://thediplomat.com/2015/10/did-china-just-hack-the-international-court-adjudicating-its-south-china-sea-territorial-claims/.

Heintschel von Heinegg, W. (2013). Territorial Sovereignty and Neutrality in Cyber Space. *89 International Law Studies*, 129.

Heriyanto, D. S. N. (2019). International Regulatory Vacuum of Cyber Espionage. *Advances in Social Science, Education and Humanities Research*, 106.

Islands of Palmas (Netherlands v US). (1928). 2 RIAA 829 838.

Laws of War: Laws and Customs of War on Land (Hague II); July 29, (1899).

Lin, H. S. (2010). Offensive Cyber Operations and the Use of Force. *Journal of National Security, Law and Policy*, 63, 78.

Lotus Case (France v Turkey). (1927). PCIJ Report Series A No 10.

Mandiant Report. (2013). State-Sponsored Cyber Espionage Projects Now Prevailed. Retrieved 30 June 2022 from http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

Mann, J. (2008). Expert: Cyber attacks on Georgia Websites Tied to Mob, Russian government. *Los Angeles times.* Retrieved 30 June 2022 from http://latimesblogs.latimes.com/technology/2008/08/experts-debate.html.

Moore, M. (2009). China Global Cyber Espionage Network, Ghost Net Penetrates 103 Countries. Retrieved 30 June 2022 from https://www.telegraph.co.uk/5071124.

Morocco's Military Justice Code (MMJC). (1956).

Nicaragua (Nicaragua v United States of America). (1986). ICJ Rep 14 para 202.

Nigeria's Manual on Laws of War (NMLW). (1994).

Philippines v. China. (2013). PCA 19; Award of 12 July 2016.

Protocols Additional to the Geneva Conventions of 12 August 1949: Additional Protocol to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts, article 46 (2).

Restatement of the Law. (1987). Third, Foreign Relations Law of the United States, section 102.

Richmond, J. A. (1998). Spies in Ancient Greece. *Greece & Rome*, 45(1), 1-18.

Roberts, A. (2001). Traditional and Modern Approaches to Customary International Law: A Reconciliation. *American Journal of International Law*, 95, 758.

Shoshan, E. (2014). Applicability of International Law on Cyber Espionage Intrusions. Ph.D thesis, Stockholm University.

SMC. (1927) amended 2007.

Smith, D. (2012). How Russia Harnesses Cyber Warfare. *Defence Dossier, American Foreign Policy Council*. Retrieved 30 June 2022 from http://www.afpc.org/files /august2012.pdf.

Smith, J. H. (2007). State Intelligence Gathering and International Law: Key Note Address. *28 Michigan Journal of International Law 544.*

Swaine, C. J. (2008). Georgia: Russia 'Conducting Cyber War. *The Telegraph*. Retrieved 30 June 2022 from http://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russiaconducting-cyberwar.html.

The Central African Republic's Penal Code (2010).

The Guardian. (24 September, 2013). *Brazilian President: US Surveillance a Breach of International Law*. Retrieved 3 July 2022 from http://www.theguardian.com/world/2013/sep/24/brazil-president-un-speech-nsa-surveillance.

The Hague Convention Respecting the Laws and Customs of War on Land, article. 29.

The MI5. (n.d.). *What is Espionage?* Retrieved 28 June 2022 from https://www.mi5.gov.uk/home/the-threats/espionage/what-isespionage.html.

The Russian Federation's Regulation on the Application of International Humanitarian Law (2001).

Uniform Code of Military Justice (UCMJ). (1951).

United Kingdom's LOAC. (2004).

United Nations Convention on the Law of the Sea. (1989). Part 2, article 2.

USMMC. (2010).

USEA. (1917).